

## Claims

WHAT IS CLAIMED IS:

- 1 1. A method for dynamically managing security associated with document  
2 collaboration, comprising:  
3 associating collaborators with different encrypted versions of a key, wherein  
4 decrypted versions of the key permit access to a document; and  
5 adding an identity service as one of the collaborators, wherein the identity  
6 service is capable of dynamically adjusting encryption formats for one or more of  
7 the collaborators' encrypted keys.
- 1 2. The method of claim 1 further comprising, dynamically adding or removing  
2 one or more of the collaborators.
- 1 3. The method of claim 1 further comprising, linking the collaborators and  
2 encrypted keys to the document as metadata defining document access and security.
- 1 4. The method of claim 1 further comprising, embedding the collaborators and  
2 encrypted keys within a portion of the document defining document access and  
3 security.
- 1 5. The method of claim 1 wherein adding further includes recognizing a select  
2 one of the collaborators as trusted to the identity service and permitting it to provide  
3 a dynamically generated public key which the identity service uses to encrypt a  
4 select one of the encrypted keys associated with the trusted collaborator.
- 1 6. The method of claim 5 wherein adding further includes inspecting a  
2 community list associated with the document to determine if the select one of the  
3 collaborators is authorized to be the trusted.

1 7. The method of claim 1 signing the document by a select one of the  
2 collaborators which modifies the document, wherein the signature is associated with  
3 a public key of the select collaborator.

1 8. The method of claim 1 further comprising:  
2 changing the key; and  
3 updating the encrypted versions of the key with the changed key.

1 9. A method for dynamically managing security associated with document  
2 collaboration, comprising:  
3 identifying a collaborator associated with a document;  
4 verifying a trust relationship between the collaborator and the document;  
5 acquiring a dynamic public key from or on behalf of the collaborator;  
6 decrypting a symmetric key which grants access to the document; and  
7 encrypting the symmetric key with the dynamic public key.

1 10. The method of claim 9 further comprising:  
2 recognizing that the collaborator has altered the document and signed the  
3 document with the dynamic public key; and  
4 communicating the dynamic public key to a plurality of other collaborators  
5 associated with the document.

1 11. The method of claim 9 wherein acquiring further includes acting as an  
2 intermediary between the collaborator and key service for purposes of acquiring a  
3 strongly rooted key pair for the collaborator, wherein a portion of that key pair is the  
4 public key and wherein another portion of that key pair is a private key which  
5 permits the collaborator to decrypt the encrypted symmetric key for purposes of  
6 accessing the document.

1 12. The method of claim 9 wherein acquiring further includes generating a non-  
2 strongly rooted private-public key pair for the collaborator.

1 13. The method of claim 9 further comprising:  
2 dynamically receiving a request from a different collaborator to access the  
3 document;  
4 inspecting a trust specification to ensure the access is permissible;  
5 receiving a public key for the different collaborator;  
6 generating a new symmetric key which includes the different collaborator,  
7 the collaborator, and other collaborators associated with the document; and  
8 encrypting the symmetric key with the public key of the different  
9 collaborator and with the dynamic public key of the collaborator and with other  
10 public keys associated with the other collaborators.

1 14. The method of claim 13 further comprising, communicating the public key  
2 of the different collaborator to the collaborator and to the other collaborators  
3 associated with the document.

1 15. The method of claim 13 wherein generating further includes generating a  
2 random new symmetric key.

1 16. The method of claim 13 wherein inspecting further includes inspecting  
2 community lists associated with the different collaborator and the document to  
3 ensure that the different collaborator can be dynamically added as a new  
4 collaborator to the document.

1 17. The method of claim 9 wherein verifying further includes authenticating the  
2 collaborator to the document according to a contract.

1 18. A dynamic collaborative document security system, comprising:  
2 a document;  
3 a list of collaborators associated with the document; and  
4 an identity service, wherein the identity service is included within the list of

5 collaborators, and wherein the identity service dynamically manages encryption of a  
6 symmetric key associated with the document and dynamically manages identities of  
7 the list of collaborators according to a trust specification, wherein access to a  
8 decrypted version of the symmetric key provides access to the document.

1 19. The dynamic collaborative document security system of claim 18 wherein  
2 each entry within the list of collaborators includes a specific encrypted version of  
3 the symmetric key, each specific encrypted version is encrypted with a specific  
4 public key of a specific collaborator included within the list of collaborators.

1 20. The dynamic collaborative document security system of claim 18 wherein  
2 the identity service changes the symmetric key and re-performs encryption when a  
3 specific collaborator is dynamically added to or dynamically removed from the list  
4 of collaborators.

1 21. The dynamic collaborative document security system of claim 18 wherein  
2 the identity service dynamically acquires a strongly rooted public-private key pair  
3 on behalf of a requesting collaborator from a keying service.

1 22. The dynamic collaborative document security system of claim 18 wherein  
2 the identity service dynamically generates a non-strongly rooted public-private key  
3 pair on behalf of a requesting collaborator.

1 23. The dynamic collaborative document security system of claim 18 wherein  
2 the identity service determines if a dynamically generated public key associated  
3 with a specific collaborator of the list of collaborators has signed the document after  
4 altering the document, and wherein if this occurs the identity service communicates  
5 the dynamically generated public key to the remaining collaborators included within  
6 the list of collaborators.

7

1 24. The dynamic collaborative document security system of claim 18 further  
2 comprising access control rights associated with each collaborator included within  
3 the list of collaborators.

1 25. A document residing in a computer readable medium, comprising:  
2 content data;  
3 a symmetric key; and  
4 a list of collaborators, each collaborator within the list associated with a  
5 specific encrypted version of the symmetric key, wherein an identity service is  
6 included within the list of collaborators, the identity service capable of dynamically  
7 adding and removing select ones of the collaborators and capable of dynamically re-  
8 encrypting the symmetric key for the select ones of the collaborators.

1 26. The document of claim 25, wherein the document is at least one of an  
2 executable program, a directory, a resource, a file, an image, and a video.

1 27. The document of claim 25, wherein the symmetric key and the list of  
2 collaborators are metadata linked with the content data.

1 28. The document of claim 25 further comprising, a trust specification that  
2 defines relationships between collaborators and the document, and wherein the trust  
3 specification drives the actions of the identity service.

1 29. The document of claim 25 further comprising, a community list which is  
2 consumed by the identity service, the community list identifying collaborators  
3 which can be dynamically added to the list of collaborators.

1 30. The document of claim 25 wherein members of the list of collaborators have  
2 been granted access control rights or edit rights to the document via the identity  
3 service which determines the access control rights or edit rights based on a trust  
4 specification for the document.

1     31.     The document of claim 25 wherein the identity service communicates a trust  
2     specification of the document dynamically to another service, and wherein that  
3     service uses the trust specification to dynamically manage access to the document.